IEEK Transactions on Smart Processing and Computing

An Identity-based Ring Signcryption Scheme: Evaluation for Wireless Sensor Networks

Gaurav Sharma, Suman Bala, and Anil K. Verma

Computer Science and Engineering Department, Thapar University, Patiala, 147004 - INDIA
{gaurav.sharma, suman.bala, akverma}@thapar.edu

***** Corresponding Author: Gaurav Sharma

Received December 13, 2012; Revised March 12, 2013; Accepted April 5, 2013; Published April 30, 2013

***Abstract*:** Wireless Sensor Networks consist of small, inexpensive, low-powered sensor nodes that communicate with each other. To achieve a low communication cost in a resource constrained network, a novel concept of signcryption has been applied for secure communication. Signcryption enables a user to perform a digital signature for providing authenticity and public key encryption for providing message confidentiality simultaneously in a single logical step with a lower cost than that of the sign-then-encrypt approach. Ring signcryption maintains the signer's privacy, which is lacking in normal signcryption schemes. Signcryption can provide confidentiality and authenticity without revealing the user's identity of the ring. This paper presents the security notions and an evaluation of an ID-based ring signcryption scheme for wireless sensor networks. The scheme has been proven to be better than the existing schemes. The proposed scheme was found to be secure against adaptive chosen ciphertext ring attacks (IND-IDRSC-CCA2) and secure against an existential forgery for adaptive chosen message attacks (EF-IDRSC-ACMA). The proposed scheme was found to be more efficient than scheme for Wireless Sensor Networks reported by Qi. et al. based on the running time and energy consumption.

***Keywords*:** Wireless sensor networks, Identity-based ring signcryption, Identity based cryptography, Anonymity

1. Introduction

A wireless sensor network [1-3] is constituted by a large number of small-sized sensor nodes with limited resources, such as communication capabilities, short coverage distance and limited processing power. With the progression of wireless sensor networks in wide-ranging applications and its adaptability to real life application scenarios, security is a prime concern in such networks. In addition, sensor based applications are often deployed in hostile environments, where the nodes can be captured by an adversary, which can lead to a revelation of data or other hidden material. Ring signcryption is one of the techniques used to address the issues of confidentiality, authentication and data integrity.

Identity-based ring signcryption is a collaboration of different security techniques, such as identity-based cryptography, ring signature and signcryption. Identity-based cryptography provides a variant to certificate-based public key cryptography; ring signature provides anonymity along with authenticity in such a way that even a verifier does not know who has signed the message but can verify that one of the ring members has signed it. Signcryption provides the encryption and signature in a single logical step.

Section 2 reviews the literature on identity-based ring signcryption. Section 3 addresses some preliminaries, which includes notations used throughout the paper, basic concepts of bilinear pairing and basic definitions of complexity assumptions. The formal model and security notions are discussed in section 4. Section 5 proposes the ID-based ring signcryption scheme. The security analysis of the proposed scheme is discussed in section 6 and is subsequently analyzed in section 7, followed by a conclusion of the proposed work.

2. Related Work

The concept of identity-based cryptography was introduced by Shamir [4] in 1984 to remove the need for the certification of public keys, which is required in a conventional public key cryptography setting. On the other hand, Shamir only proposed an ID-based signature and left the ID-based encryption as an open problem. Boneh et al. [5] presented the first Identity Based Encryption (IBE) scheme that uses bilinear maps (the Weil or Tate pairing) over super singular elliptic curves. Rivest et al. [6] introduced a ring signature, which is a group oriented signature with privacy concerns: a user can anonymously sign a message on behalf of a group of spontaneously conscripted users, without managers including the actual signer. Zheng et al. [7] proposed the first ID-based ring signature scheme with bilinear parings. Yuliang Zheng [8] introduced the concept of public key signcryption, which fulfils both functions of the digital signature and public key encryption in a logically single step, and with a lower cost than that required by the sign-then-encrypt approach. On the other hand, Zheng did not prove any security notions, which was further proposed by Baek et al. [9], and described a formal security model in a multi-user setting.

Xinyi Huang [10] combined the concepts of an ID-based ring signature and signcryption together as identity-based ring signcryption. They provided formal proof of their scheme with the chosen ciphertext security (IND-IDRSC-CCA) under the Decisional Bilinear Diffie-Hellman assumption. On the other hand, Huang et al.'s [11] scheme is computationally inefficient because the number of pairing computations grows linearly with the group size. Huang et al.'s scheme needs n+4 pairing computations, where n denotes the size of the group. The scheme lacks anonymity and had a key escrow problem because the scheme was based on ID-PKC. Wang et al. [12] eliminated the key escrow problem in [10] by proposing a verifiable certificate-less ring signcryption scheme and gave formal security proof of the scheme in a random oracle model. On the other hand, this scheme also requires n+4 pairing computations. The problem of ID-based ring signcryption schemes is that they are derived from bilinear pairings, and the number of pairing computations grows linearly with the group size. Zhu et al. [13] solved the above problem. They proposed an efficient ID-based ring signcryption scheme, which only takes four pairing operations for any group size. Zhu et al. [14] proposed an ID-based ring signcryption scheme, which offers savings in the ciphertext length and computational cost. The other schemes include those reported by Li et al. [15, 16], Yu et al. [17] and Zhang et al. [18]. Selvi et al. [19] proved that Li et al.’s [15] and Zhu et al.’s scheme [13] are not secure against an adaptive chosen ciphertext attack, whereas Zhu et al.’s [14] scheme and Yu et al.’s [17] scheme are not secure against a chosen plaintext attack. Qi et al. [20] proved that their scheme has the shortest ciphertext and is much more efficient than Huang et al.’s [10] and Selvi et al.’s [19] scheme. Selvi et al. [21] proved that Zhang et al.’s [22] scheme is insecure against confidentiality, existential unforgeability and anonymity attacks. Zhou [23] presented an efficient identity-based ring signcryption scheme in the standard model. This paper presents the security notions and an evaluation of an ID-based ring signcryption scheme [27] for wireless sensor networks. A comapartive analysis of the proposed scheme has been done based on the operations carried out in an algorithm and the size of the ciphertext. Further, the scheme has been evaluated on the basis of running time and energy consumption with Qi et al.‘s [20] scheme.

3. Preliminaries

This section provides a brief review of some preliminaries that will be used throughout the paper.

3.1 Notations Used

The following notations have been made in common for all existing schemes and Table 1 summarizes the notations used in this paper.

3.2 Basic Concepts on Bilinear Pairing

Let G_1 be a cyclic additive group generated by P of prime order q, and G_2 be a cyclic multiplicative group of the same order q. Let a and b be the elements of Z_q^*. Assume that the discrete logarithm problem (DLP) in both G_1 and G_2 is hard. Let $\hat{e}: G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing with the following properties shown in Table 2.

3.3 Complexity Assumptions

- **Bilinear Diffie-Hellman Problem (BDHP):** Given two groups G_1 and G_2 of the same prime order q, a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the BDHP in $(G_1, G_2, \hat{e})$ is to compute $\hat{e}(P,P)^{abc}$ given (P, aP, bP, cP);
- **Decisional Bilinear Diffie-Hellman Problem (DBDHP):** Given $(P, aP, bP, cP) \in G_1^4$ for unknown $a,b,c \in Z_q^*$ and $h \in G_2$, to decide whether $h \overset{?}{=} \hat{e}(P,P)^{abc}$ holds;
- **Computational Bilinear Diffie-Hellman Problem (CBDHP):** Given $(P, aP, bP, cP) \in G_1^4$ for unknown $a,b,c \in Z_q^*$, the CBDHP in G_1 is to calculate $\hat{e}(P,P)^{abc}$ $\in G_2$. The advantage of any probabilistic polynomial time algorithm A in solving the CBDHP in G_1 is defined as: $Adv_A^{CBDH} = \Pr\left[A(P, aP, bP, cP) = \hat{e}(P,P)^{abc} \mid a,b,c \in Z_q^*\right]$. The CBDH Assumption is that for any probabilistic polynomial time algorithm A, the advantage Adv_A^{CBDH} is negligibly small;
- **Computational Diffie-Hellman Problem (CDHP):** Given $(P, aP, bP) \in G_1^3$, for unknown $(P, aP, bP) \in G_1^3$, the CDHP in G_1 is to compute abP. The advantage of any probabilistic polynomial time algorithm A in solving the CDHP in G_1 is defined as $Adv_A^{CDH} =$ $\Pr\left[A(P, aP, bP) = abP \mid a,b \in Z_q^*\right]$. The *CDH Assumption* is that for any probabilistic polynomial time algorithm A, the advantage Adv_A^{CDH} is negligibly small.

Table 1. Notations Used.

k : security parameter *params:* systems' public parameter generated by PKG *t*: secret key generated by PKG G_1 : cyclic additive group generated by P of prime order $q > 2^k$ G_2 : cyclic multiplicative group generated by P of prime order $q > 2^k$ $P \in G_1$: random generator P_{pub} : public key of PKG Z_q^* : multiplicative group modulo q A : probabilistic polynomial time algorithm $\{0,1\}^*$: string with arbitrary length $\{0,1\}^l$: string with length l $\mathcal{L} = \{ID_1,...,ID_n\}$: Ring of user's identities ε : the advantage for the adversary in the game $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$, $\mathcal{O}_{Keygen}$, $\mathcal{O}_{Signcrypt}$, $\mathcal{O}_{Unsigncrypt}$: oracles L : List maintained by a challenger	$\hat{e}: G_1 \times G_1 \to G_2$ is a bilinear pairing ID_i : user identity S_i : private key of user i Q_i : public key of user i S: sender R: receiver U_i : user $\mathcal{L}$: group of ring members σ : Signcrypted ciphertext $\mathcal{C}$: signcrypted ciphertext n_1: length of the message n: number of users in the group $\mathcal{A}$: Adversary $\mathcal{C}$: Challenger $m \in_R M$: message, M : message space

Table 2. Properties of Bilinear Mapping.

Bilinearity	Non-degeneracy	Computability
$\forall\ P,Q,R \in_R G_1$ $\hat{e}(P+Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$ $\hat{e}(P,Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$ In particular, for any $a,b \in Z_q^*$ $\hat{e}(aP,bP) = \hat{e}(P,P)^{ab} = \hat{e}(P,abP) = \hat{e}(abP,P)$	$\exists\ P,Q,\in G_1 \ni \hat{e}(P,Q) \neq I_{G_2}$, where I_{G_2} is the identity of G_2	$\forall\ P,Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P,Q)$

Table 3. Generic Identity Based Ring Signcryption Scheme.

Algorithm	Description
Setup	For a given parameter k, a trusted private key generator generates system's public parameters *params* and its corresponding master secret key t, which is kept secret.
Keygen	For a given user identity ID_i, PKG computes private key S_i by using *params* and t and transmits S_i to ID_i via secure channel.
Signcrypt	For sending a message m from sender to a receiver with identity ID_R, senders' private key S_S, and a group of ring members $\{U_i\}_{i=1 \text{ to } n}$ with identities $\mathcal{L} = \{ID_1,...,ID_n\}$, sender computes a ciphertext.
Unsigncrypt	For retrieving a message m, if $\mathcal{C}$ is a valid ring signcryption of m from the ring $\mathcal{L}$ to ID_R or 'invalid', if $\mathcal{C}$ is an invalid ring signcryption.
Consistency	An identity based ring signcryption scheme is said to be consistent iff $\Pr\left[\mathcal{C} \leftarrow signcrypt(m,\mathcal{L},S_S,ID_R), m \leftarrow unsigncrypt(\mathcal{C},\mathcal{L},S_R)\right] = 1$

4. Formal Model of Identity-Based Ring Signcryption

This section discusses the formal model of identity-based ring signcryption, which includes a generic scheme and security notions.

4.1 Generic Scheme

A generic ID-based ring signcryption scheme consists of five algorithms: Setup, Keygen, Signcrypt, Unsigncrypt and Consistency. Table 3 provides a description of these algorithms.

4.2 Security Notion

Baek et al. [9] presented a formal security definition of signcryption in 2002. The security of an ID-based signcryption scheme was first defined by Malone-Lee [24], which satisfies the indistinguishability against adaptive chosen ciphertext attacks and unforgeability against adaptive chosen message attacks.

- **Confidentiality:** An identity-based ring signcryption (IRSC) is indistinguishable against adaptive chosen ciphertext attacks (IND-IRSC-CCA2), if there is no polynomially bounded adversary $\mathcal{A}$ with a non-negligible advantage in the following game:
  1. *Setup Phase* - The challenger $\mathcal{C}$ runs the setup algorithm with the security parameter k as an input and sends the system parameters $params$ to the adversary $\mathcal{A}$ and keeps the master private key t secret.
  2. *Phase-I* - The adversary $\mathcal{A}$ performs polynomially-bounded number of queries to the oracles provided to $\mathcal{A}$ by $\mathcal{C}$. The description of the queries in the phase-I are listed as follows:
     a. *Keygen Queries: The adversary $\mathcal{A}$ produces an identity ID_i corresponding to $\mathcal{L}_i$ and receives the private key S_i corresponding to ID_i.*
     b. *Signcrypt Queries* $(m, \mathcal{L}, S_A, ID_R)$: $\mathcal{A}$ produces a message $m \in_R M$, a user group $\mathcal{L} = \{ID_i\}_{(i=1 \text{ to } n)}$, a sender identity ID_A and a receiver identity ID_R to the challenger $\mathcal{C}$. $\mathcal{C}$ then returns the signcrypted ciphertext $\mathcal{C} = (m, \mathcal{L}, S_A, ID_R)$ to $\mathcal{A}$, where private key S_A is generated by querying the *Keygen* oracle.
     c. *Unsigncrypt Queries* $(\mathcal{C}, \mathcal{L}, S_R)$ *:* $\mathcal{A}$ produces a sender group $\mathcal{L} = \{ID_i\}_{(i=1 \text{ to } n)}$, a receiver identity ID_R, and a ring signcryption $\mathcal{C}$. $\mathcal{C}$ generates the private key S_R by querying the Key Extraction Oracle. $\mathcal{C}$ unsigncrypts $\mathcal{C}$ using S_R and returns m if $\mathcal{C}$ is a valid ring signcryption of m from the ring $\mathcal{L}$, to ID_R, else outputs 'Invalid'.
  3. $\mathcal{A}$ queries the various oracles adaptively, i.e. the current oracle requests may depend on the response to the previous oracle queries.
  4. *Challenge*: $\mathcal{A}$ chooses two plaintexts $\{m_0, m_1\} \in M$ of equal length, a set of $\bar{n}$ users $\mathcal{L}^* = \{ID_i^*\}_{(i=1 \text{ to } \bar{n})}$ and a receiver identity ID_R^*, and sends them to $\mathcal{C}$. $\mathcal{A}$ should not have queried the private key corresponding to ID_R^* in Phase-I. $\mathcal{C}$ now chooses a bit $b \in_R \{0,1\}$ and computes the challenge ring signcryption $\mathcal{C}^*$ of m_b and sends $\mathcal{C}^*$ to $\mathcal{A}$.
  5. *Phase-II*: $\mathcal{A}$ performs polynomially-bounded number of requests just like the Phase-I, with the restrictions that $\mathcal{A}$ cannot make Key Extraction query on ID_R^* and should not query for unsigncryption query on $\mathcal{C}^*$. The ID_R^* can be included as a ring member in $\mathcal{L}^*$, but $\mathcal{A}$ cannot query the private key of ID_R^*.
  6. *Guess* - Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$. The success probability is defined as $Succ_A^{IND\text{-}IRSC\text{-}CCA2}(k) = \frac{1}{2} + \varepsilon$, where, ε is called the advantage for an adversary in the above game.
- **Unforgeability:** An identity-based ring signcryption scheme (IRSC) is said to be existentially unforgeable against adaptive chosen message attack (EUF-IRSC-CMA), if no polynomially bounded adversary has a non-negligible advantage in the following game:
  1. *Setup Phase*: The challenger $\mathcal{C}$ runs the Setup algorithm with the security parameter k to generate the system parameters $params$ and the master secret key t. $\mathcal{C}$ gives $params$ to adversary $\mathcal{A}$ and keeps t secret.
  2. *Training Phase*: $\mathcal{A}$ performs polynomially-bounded number of queries, as described in Phase-I of the confidentiality game.
  3. *Existential Forgery*: Finally, $\mathcal{A}$ produces a new triple $(\mathcal{L}^*, ID_R^*, \mathcal{C}^*)$ (i.e. this triple that was not produced as output by the signcryption oracle), where the private keys of the users in ring $\mathcal{L}^*$ were not queried during the training phase. $\mathcal{A}$ wins the game if the result of the Unsigncryption $(\mathcal{L}^*, ID_R^*, \mathcal{C}^*)$ is not 'Invalid', i.e. $\mathcal{C}^*$ is a valid signcryption of some message $m \in M$.
  4. ID_R^* can also be member of the ring $\mathcal{L}$ and in that case, the private key of ID_R^* should not be queried by $\mathcal{A}$. On the other hand, if $ID_R^* \notin \mathcal{L}^*$, $\mathcal{A}$ may query the private key of ID_R^*.
  5. The security model described here deals with insider security because the adversary is assumed to have access to the private key of the receiver of a signcryption used for the generation of $\mathcal{C}^*$. This means that the unforgeability is preserved even if a receiver′s private key is compromised.
- **Anonymity:** An ID-based ring signcryption scheme is unconditionally anonymous if for any group of n members $(n \geq 3)$ with identities $\mathcal{L} = \{ID_i\}_{(i=1 \text{ to } n)}$, any message m and Ciphertext $\mathcal{C}$, any adversary cannot identify the actual signcrypter with a probability better than a random guess. That is, $\mathcal{A}$ outputs the identity of actual signcrypter with probability $1/n$ if he/she is not a member of $\mathcal{L}$, and with a probability $1/(n-1)$ if he/she is a member of $\mathcal{L}$.
- **Public Verifiability:** An ID-based ring signcryption scheme is publicly verifiable if given a ciphertext $\mathcal{C}$, ring $\mathcal{L}$, and receiver R, anyone can verify that $\mathcal{C}$ is a valid signcryption by some member of the ring $\mathcal{L}$ to the specified receiver R, without knowing the receiver's private key.

5. Proposed Scheme

This section present the proposed Identity-Based Ring signcryption Scheme. This scheme has the following four algorithms:

1. *Setup* (k): Given a security parameter k, a trusted

private key generator (PKG) generates the system's public parameters *params* and the corresponding master secret key t that is kept secret by PKG.

a. The trusted authority randomly chooses $t \in_R Z_q^*$ keeps it as a master key and computes the corresponding public key $P_{pub} = tP$.

b. Let $(G_1,+)$ and $(G_2,*)$ be two cyclic groups of prime order $q > 2^k$ and a random generator $P \in G_1$.

c. $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing.

d. Choose Hash Functions

i. $H_1: \{0,1\}^* \rightarrow G_1$

ii. $H_2: G_2 \rightarrow \{0,1\}^l$

iii. $H_3: \{0,1\}^* \rightarrow Z_q^*$

iv. $H_4: \{0,1\}^* \rightarrow \{0,1\}^l$

e. The public parameters are:

$params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$.

2. *Keygen* (ID_i): Given a user identity ID_i of user U_i , the PKG, using the public key computes the parameters *params* and the master secret key t , computes the corresponding private key S_i , and transmits it to ID_i in a secure way as follows:

a. The public key is computed as $Q_i = H_1(ID_i)$.

b. The corresponding private key $S_i = tQ_i$.

c. PKG sends S_i to the user U_i via a secure channel.

3. *Signcrypt*: Let $\mathcal{L} = \{ID_1,...,ID_n\}$ be a set of n ring members, such that $ID_S \in \mathcal{L}$. ID_R may or may not be in $\mathcal{L}$. The sender runs this algorithm to send a message $m \in M$, where M is a message space, to a receiver with identity ID_R . The sender's private key, S_S , outputs a ring signcryption $\mathcal{C}$ as follows:

a. Choose a random number $r \in_R Z_q^*$ and $m^* \in_R M$. And calculate $R_0 = rP$, $R = e\left(rP_{pub}, Q_R\right)$, $k = H_2\left(R\right)$, $\mathcal{C}_1 = m^* \oplus k$

b. Choose $R_i \in G_1 \quad \forall\ i = \{1,2,...,n\} \setminus \{S\}$ and calculate $h_i = H_3(m \| \mathcal{L} \| R_i \| R_0)$.

c. Choose $r_S \in_R Z_q^* \quad \forall\ i = S$.

Calculate $R_S = r_S Q_S - \sum_{i \neq S} \left(R_i + h_i Q_i\right)$,

$h_S = H_3(m \| \mathcal{L} \| R_S \| R_0)$,

$V = \left(h_S + r_S\right) S_S$,

$\mathcal{C}_2 = \left(m \| r_S \| V\right) \oplus H_4(m^* \| R_0)$.

d. Finally the sender outputs the ciphertext as $\sigma = (\mathcal{L}, R_0, R_1, ..., R_n, \mathcal{C}_1, \mathcal{C}_2)$ to the receiver.

4. *Unsigncrypt*: This algorithm is executed by a receiver ID_R . This algorithm takes the ring signcryption, σ , the ring members $\mathcal{L}$ and the private key S_R , as input and produces the plaintext m , if σ is a valid ring signcryption of m from the ring $\mathcal{L}$ to ID_R or 'invalid', if σ is an invalid ring signcryption as follows:

a. Calculate $R' = e(R_0, S_R)$, $k' = H_2(R')$, $m'^* = \mathcal{C}_1 \oplus k'$

b. Recover m' , V' as $\left(m' \| r_S \| V'\right) = \mathcal{C}_2 \oplus H_4(m'^* \| R_0)$.

c. Calculate $h_i' = H_3(m' \| \mathcal{L} \| R_i \| R_0) \ \ \forall\ i = \{1,2,...,n\}$.

Check if $e(P, V') \overset{?}{=} e\left(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)\right)$. If the check succeeds accept m , else return $\perp$.

6. Security Analyses of the Proposed Scheme

This section discusses the correctness of the signcrypted ciphertext and provides a security analysis of the proposed scheme.

6.1 Correctness

In this section, a proof of the correctness is provided. The verification equations will hold if the ciphertext $\mathcal{C}$ has been generated correctly, i.e. $e(P, V') \overset{?}{=} e\left(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)\right)$.

L.H.S.

$$e\left(P,V\right) = e\left(P, \left(h_S + r_S\right) S_S\right) = e\left(P, \left(h_S + r_S\right) tQ_S\right)$$
$$= e\left(tP, h_S Q_S + R_S + \sum_{i=1, i \neq S}^{n} \left(R_i + h_i Q_i\right)\right)$$
$$= e\left(P_{pub}, \sum_{i=1}^{n} \left(R_i + h_i Q_i\right)\right)$$

6.2 Security Analysis

In this section, security analysis of the proposed scheme is shown. The security is analyzed in terms of confidentiality and unforgeability.

Proof of Confidentiality

Theorem: If an IND-IRSC-CCA2 adversary $\mathcal{A}$ has an advantage ε against an IRSC scheme, asking hash queries to random oracles $\mathcal{O}_{H_i}\ \left(i = 1,2,3,4\right)$, q_e extract queries ($q_e = q_{e_1} + q_{e_2}$, where q_{e_1} and q_{e_2} are the number of extract queries in the first phase and second phase respectively), q_{sc} signcryption queries and q_{us} unsigncryption queries, then there exist an algorithm $\mathcal{C}$ that solves the CBDHP with the advantage $\varepsilon\left(\frac{1}{q_{H_1} q_{H_2}}\right)$.

Proof: The challenger $\mathcal{C}$ is challenged with an instance (P, aP, bP, cP, h) of the Decisional Bilinear **Diffie-Hellman Problem.** His goal is to determine if $h = (P,P)^{abc}$ or not. Assume that there is an adversary $\mathcal{A}$ capable of breaking the IND-IRSC-CCA2 security with a non-negligible advantage. $\mathcal{C}$ makes use of $\mathcal{A}$ to solve the CBDHP instance. $\mathcal{C}$ simulates the system with the various oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$, $\mathcal{O}_{Keygen}$, $\mathcal{O}_{Signcrypt}$, $\mathcal{O}_{Unsigncrypt}$ and allows $\mathcal{A}$ to make a polynomially-bounded number of queries, adaptively to these oracles. The game between $\mathcal{C}$ and $\mathcal{A}$ is as follows:

1. *Setup Phase*: The challenger $\mathcal{C}$ runs the Setup algorithm with the security parameter k and generates the system parameters *params* using the master secret key t as follows:
   a. $\mathcal{C}$ takes two groups G_1 and G_2, and a generator $P \in G_1$.
   b. Calculates the master public key $P_{pub} = tP$.
   c. Modeling the Hash functions as random oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$ and $\mathcal{O}_{H_4}$.
   d. Selecting a bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$.
   e. Delivering $(G_1, G_2, e, P, P_{pub})$ to $\mathcal{A}$.
2. *First Phase*: To handle the oracle queries, $\mathcal{C}$ maintains three lists $L_i\left(i=1,2,3,4\right)$, which keeps track of the responses given by $\mathcal{C}$ to the corresponding oracle ($\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$) queries. $\mathcal{A}$ adaptively queries the various oracles in the first phase, which are handled by $\mathcal{C}$ as given below:
   a. $\mathcal{O}_{H_1}$ Query: Assume that $\mathcal{A}$ queries the $\mathcal{O}_{H_1}$ oracle with distinct identities in each query. There is no loss of generality due to this assumption because if the same identity is repeated, the oracle consults the list L_1 and gives the same response. Therefore, it is assumed that $\mathcal{A}$ asks q_{H_1} distinct queries for q_{H_1} distinct identities. Among the q_{H_1} identities, a random identity needs to be selected as the target identity and done as follows.
      i. $\mathcal{C}$ selects a random index, j where $1 \le j \le q_{H_1}$. $\mathcal{C}$ does not reveal j to $\mathcal{A}$. When $\mathcal{A}$ asks the j^{th} query on ID_j, $\mathcal{C}$ decides to fix ID_j as the target identity for the challenge phase. $\mathcal{C}$ responds to $\mathcal{A}$ as follows:
         - If it is the j^{th} query, then $\mathcal{C}$ sets $Q = bP$, returns Q_j as the response to the query and stores $(ID_j, Q_j, *)$, in the list L_1. Here, $\mathcal{C}$ does not know b. $\mathcal{C}$ is simply using the value bP given in the instance of the CBDHP.
         - For all other queries, $\mathcal{C}$ chooses $x_i \in_R Z_q^*$ and sets $Q_i = x_i P$ and stores $\langle ID_i, Q_i, x_i \rangle$ in the list L_1.
      ii. $\mathcal{C}$ returns Q_i to $\mathcal{A}$.
   b. $\mathcal{O}_{H_2}$ *Query*: When $\mathcal{A}$ makes a query to this oracle with R as an input, $\mathcal{C}$ retrieves h_2 from list L_2 and returns h_2 to $\mathcal{A}$, if the tuple exists in the list; else, chooses a new h_2 randomly, stores $\langle R, h_2 \rangle$ in L_2 and returns h_2 to $\mathcal{A}$.
   c. $\mathcal{O}_{H_3}$ *Query*: When $\mathcal{A}$ makes a query to this oracle with $(m \,\|\, \mathcal{L} \,\|\, R_i \,\|\, R)$ as input, $\mathcal{C}$ retrieves $h_i^{(3)}$ from list L_3 and returns $h_i^{(3)}$ to $\mathcal{A}$; else, chooses a new $h_i^{(3)} \in_R Z_q^*$ randomly, stores $\langle m \,\|\, \mathcal{L} \,\|\, R_i \,\|\, R, h_i^{(3)} \rangle$, in the list L_3 and returns $h_i^{(3)}$ to $\mathcal{A}$.
   d. $\mathcal{O}_{H_4}$ *Query*: When $\mathcal{A}$ makes a query to this oracle with $(m^* \,\|\, R_0)$ as input, $\mathcal{C}$ retrieves h_4 from list L_4 and returns h_4 to $\mathcal{A}$, if the tuple exists in the list; else, chooses a new h_4 randomly, stores $\langle m^* \,\|\, R_0, h_4 \rangle$ in L_4 and returns h_4 to $\mathcal{A}$.
   e. $\mathcal{O}_{Keygen}$ *Query*: Upon obtaining a request for the private key of user U_i with identity ID_i, $\mathcal{C}$ aborts if $ID_i = ID_j$. Else, $\mathcal{C}$ retrieves Q_i, x_i from list L_1 and returns $S_i = x_i tP = tQ_i$.
   f. $\mathcal{O}_{Signcrypt}$ *Query*: $\mathcal{A}$ chooses a message m, a set of n potential senders and forms an ad-hoc group $\mathcal{L}$ by fixing a sender ID_S and a receiver ID_R and sends them to $\mathcal{C}$. To respond correctly to the signcryption query on the plaintext m chosen by $\mathcal{A}$, $\mathcal{C}$ proceeds according to the signcryption algorithm when $ID_S \ne ID_j$. This is possible as $\mathcal{C}$ knows the private key S_S of the sender ID_S and runs $\mathcal{O}_{Signcrypt}\left(m, \mathcal{L}, Q_R\right)$ to signcrypt a message on behalf of the group. If the sender's identity $ID_S = ID_j$, $\mathcal{C}$ proceeds according to the signcryption algorithm (i.e. when $\mathcal{C}$ does not know the private key corresponding to ID_S). Finally, $\mathcal{C}$ returns the result ciphertext σ to $\mathcal{A}$.
   g. $\mathcal{O}_{Unsigncrypt}$ *Query*: For a unsigncryption query on a ciphertext $\sigma = (\mathcal{L}, R_0, R_1, ..., R_n, \mathcal{C}_1, \mathcal{C}_2)$ between a user group $\mathcal{L}$ and a receiver with identity ID_R. If $ID_R = ID_j$, $\mathcal{C}$ always notifies $\mathcal{A}$ that the ciphertext is invalid. If $ID_R \ne ID_j$, $\mathcal{C}$ runs the $\mathcal{O}_{H_3}$ simulation algorithm to obtain $h_i' = H_3(m' \,\|\, \mathcal{L} \,\|\, R_i \,\|\, R')$ for $i = \{1, 2, ..., n\}$. $\mathcal{C}$ then checks if $e(P, V') \stackrel{?}{=} e\left(P_{pub}, \sum_{i=1}^{n}(R_i + h_i Q_i)\right)$ holds. If it does not hold, $\mathcal{C}$ rejects the ciphertext. Otherwise, $\mathcal{C}$ calculated $R' = e(R_0, S_R)$. $\mathcal{C}$ can obtain S_R from the $\mathcal{O}_{Keygen}$ algorithm because $ID_R \ne ID_j$. Finally, $\mathcal{C}$ computes m and returns to $\mathcal{A}$.
3. *Challenge Phase*: $\mathcal{A}$ chooses two equal length plaintexts $m_0, m_1 \in M$ the set of ring members $\mathcal{L}^* = \left\{ID_1, ..., ID_n\right\}$, a sender $ID_S \in \mathcal{L}^*$ and a receiver

ID_R on which $\mathcal{A}$ wants to be challenged and sends them to $\mathcal{C}$. $\mathcal{A}$ should not have queried the private key corresponding to ID_R in the first phase. $\mathcal{C}$ aborts, if $ID_R \neq ID_j$, else $\mathcal{C}$ chooses a bit $\delta \in_R \{0,1\}$ and computes the challenge ring signcryption σ^* of m_δ.

4. *Second Phase*: Upon receiving the challenge ring signcryption σ^* $\mathcal{A}$ is allowed to interact with $\mathcal{C}$ as in the first phase. This time, $\mathcal{A}$ is not given access to the private key of ID_R and is also restricted from querying the decryption oracle for the ring unsigncryption of σ^*.
5. *Guess*: After the second phase, $\mathcal{A}$ returns its guess. $\mathcal{C}$ ignores the answer from $\mathcal{A}$, picks a random tuple $\langle R, h_2 \rangle$ from list L_2 and returns the corresponding R as the solution to the CBDH problem instance. Because the challenge ciphertext σ^* given to $\mathcal{A}$ is distributed randomly in the ciphertext space, $\mathcal{A}$ cannot gain any advantage in this simulation. Therefore, any adversary that has an advantage ε in the real IND-IBRSC-CCA2 game must necessarily recognize with probability at least ε that the challenge ciphertext provided by $\mathcal{C}$ is incorrect. For $\mathcal{A}$ to find that σ^* is not a valid ciphertext, $\mathcal{A}$ should have queried the $\mathcal{O}_{H_2}$ oracle with $R' = e\left(R_0^*, S_j\right)$. Here, S_j is the private key of the target identity and it is $aQ_j = abP$. In addition, $\mathcal{C}$ sets $R_0^* = cP$. Hence, $R' = e\left(R_0^*, S_j\right) = e\left(cP, abP\right) = e(P,P)^{abc}$. Therefore, one of the entries in list L_2 should be the value $e(P,P)^{abc}$. With a probability of $1/q_{H_1}$, the value of R' chosen by $\mathcal{C}$ from list L_2 will be the solution to the CBDHP. Now, the probability of success of $\mathcal{C}$ is assessed. The events in which $\mathcal{C}$ aborts the IND-IRSC-CCA2 game are $PR[\mathcal{C}(P, aP, bP, cP \mid a,b,c \in_R Z_q^*)$ $= e\left(P,P\right)^{abc}] = \varepsilon\left(\dfrac{1}{q_{H_1} q_{H_2}}\right)$.

Proof of Unforgeability

Theorem: An identity-based ring signcryption scheme (IRSC) is said to be existentially unforgeable against an adaptive chosen message attack (EUF-IRSC-CMA), and against any polynomially-bounded adversary $\mathcal{A}$ under the random oracle model if the CDHP is hard.

Proof: The challenger $\mathcal{C}$ is challenged to solve an instance $(P, aP, bP) \in G_1$ of the CDHP with the help of the adversary $\mathcal{A}$. His objective is to determine abP. When the challenger receives the instance from the adversary $\mathcal{A}$, $\mathcal{C}$ begins the interaction with $\mathcal{A}$ to calculate the value of $abP \in G_1$. The challenger will set the various random oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$, $\mathcal{O}_{Keygen}$, $\mathcal{O}_{Signcrypt}$, $\mathcal{O}_{Unsigncrypt}$ and allows $\mathcal{A}$ to adaptively ask polynomially bounded number of queries to the oracles. The game between $\mathcal{C}$ and $\mathcal{A}$ as follows:

1. *Setup Phase*: The challenger $\mathcal{C}$ runs the Setup algorithm with the security parameter k and generates the system parameters *params* with the help of the master secret key t as follows:
   a. $\mathcal{C}$ takes two groups, G_1 and G_2, and a generator, $P \in G_1$.
   b. Calculates the master public key $P_{pub} = tP$.
   c. Modeling the Hash functions as random oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$ and $\mathcal{O}_{H_4}$.
   d. Selecting a bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$.
2. *Training Phase*: $\mathcal{A}$ performs a polynomially-bounded number of queries on various oracles. The queries may be Hash Queries, Extract Queries, Signcrypt Queries and Unsigncrypt Queries with no restrictions, handled by the challenger $\mathcal{C}$.
3. *Existential Forgery*: $\mathcal{A}$ produces a forged signcryption $\sigma^* = (\mathcal{L}^*, R_0^*, R_1^*, R_2^*, ..., R_n^*, \mathcal{C}_1^*, \mathcal{C}_2^*)$ on the message m^*, where the private keys of the users who are in the group $\mathcal{L}^*$ were not queried in the training phase. This means that σ^* was not produced by $\mathcal{O}_{Signcrypt}$ as an output for the ring signcryption query on the message m^* with a group of user's identity $\mathcal{L}^*$ and the receiver's identity ID_R. $\mathcal{C}$ aborts if $\mathcal{L}^*$ does not contain the target identity. Otherwise, $\mathcal{C}$ can unsigncrypt and verify the validity of the forged ring signcryption σ^*.
4. If the ring signature of the forged ring signcryption passes the verification then $\mathcal{C}$ will be able to generate one more valid ring signcryption from $\sigma^* = (\mathcal{L}^*, R_0^*, R_1^*, R_2^*, ..., R_n^*, \mathcal{C}_1^*, \mathcal{C}_2^*)$ known as $\sigma^* = (\mathcal{L}^*, R_0^*, R_1^*, R_2^*, ..., R_n^*, \mathcal{C}_1^*, \mathcal{C}_2^*)$ using the oracle replay technique and applying the extended version of a forking lemma applicable for ring signatures. Obviously, $\mathcal{A}$, who is capable of generating a valid ring signcryption, will be able to generate a new valid ring signcryption again with the same randomness again. Upon receiving two valid ring signcryption on m^*, $\mathcal{C}$ will be able to retrieve $S_S = abP$ as follows:
5. Because, V^* and V' have the same randomness, so we compute $V^* = \left(h_S^* + r_S\right) S_S$ and $V' = \left(h_S' + r_S\right) S_S$ are calculated. Hence, $V^* - V' = \left(h_S^* - h_S'\right) S_S$. As, $\mathcal{C}$ knows the hash values h_{SS}^* and h_S', $\mathcal{C}$ can calculate $S_S = \left(V^* - V'\right)\left(h_S^* - h_S'\right)^{-1}$. This means, $\mathcal{C}$ can calculate abP. In other words, $\mathcal{C}$ is capable of solving CDHP, but this is not possible. Hence, it shows the proposed scheme is secure against EUF-IBRSC-CMA.

Table 4. Efficiency Comparison.

Scheme	Year	Ciphertext size	Signcryption				Unsigncryption			
			Pairing	G_1 Add	G_1 Mult	G_2 Mult	Pairing	G_1 Add	G_1 Mult	G_2 Mult
X. Huang [10]	2005	$\|U\|+2n_1+2\|G_1\|+n\|G_2\|+nZ_q^*$	n+2	2n-2	2n+2	1	3	n-1	n	n
L.Wang [12]	2007	$\|U\|+3n_1+2\|G_1\|+n\|G_2\|+nZ_q^*$	n+2	2n-2	2n+2	1	2n+3	n-1	n	n
Z. Zhu [13]	2008	$2n_1+(n+2)\|G_1\|$	1	2n-2	n+4	0	3	2n-1	n	0
L. Zhu [14]	2008	$n_1+(n+1)\|G_1\|$	1	2n-2	3n+2	0	3	2n-1	n	0
F. Li [15]	2008	$\|U\|+n_1+(n+2)\|G_1\|$	1	2n-2	2n+2	0	3	2n-1	n	0
F. Li [16]	2008	$\|U\|+n_1+(n+2)\|G_1\|$	1	2n-3	2n+2	0	3	2n-1	n	0
Y. Yu [17]	2008	$\|U\|+n_1+(n+2)\|G_1\|+nZ_q^*$	1	2n-2	n+3	0	3	2n-1	n	0
J. Zhang [18]	2009	$n_1+(n+2)\|G_2\|$	1	5n-4	5n+1	0	4	2n-1	n	1
S. Selvi [19]	2010	$\|U\|+2n_1+(n+3)\|G_1\|$	1	2n-2	n+5	0	5	2n-1	n	0
Z. Qi [20]	2010	$\|U\|+n_1+(n+2)\|G_1\|$	1	2n-2	2n+2	0	3	2n-1	n	0
Proposed Scheme		$\|U\|+2n_1+(n+1)\|G_1\|$	1	2n-2	n+4	0	3	2n-1	n	0

Table 5. Number of nodes vs. Running Time/Energy Consumption.

	Number of pairing	Number of point multiplications	Number of nodes (in the ring)	MICA2		T-mote sky	
				Running time (s)	Energy consumption (mJ)	Running time (s)	Energy consumption (mJ)
Z.Qi. Scheme [20]	4	3n+2	5	80.56	1899.60	38.68	400.34
			15	145.36	3427.59	69.88	723.26
			30	242.56	5719.56	116.68	1207.64
			50	372.16	8775.53	179.08	1853.48
Proposed Scheme	4	2n+4	5	74.08	1746.81	35.56	368.05
			15	117.28	2765.46	56.36	583.33
			30	182.08	4293.45	87.56	906.25
			50	268.48	6330.76	129.16	1336.81

Running Time = (*Number of Pairings* x *Computation time of Pairing*)
+ (*Number of Point Multiplications* x *Computation time of Point Multiplication*)

Total Energy Consumption =*Voltage Level* x *Current* x *Running Time*

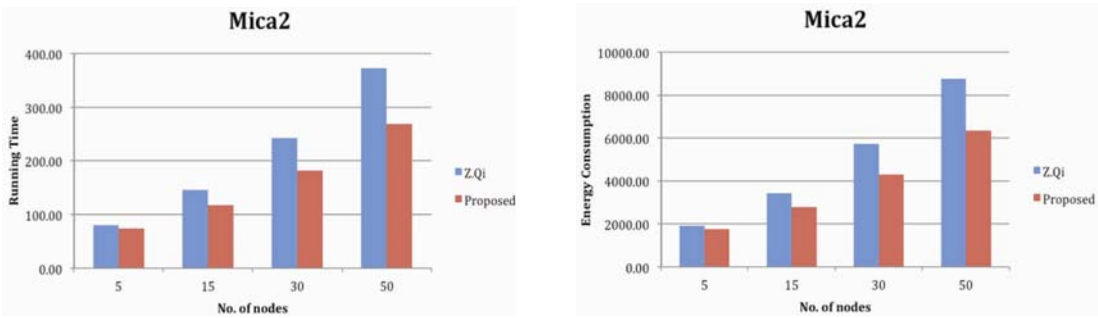
Fig. 1. Formulae for the running time and energy consumption [25].

7. Efficiency Analysis

The major parameters involved in the identity based ring signcyption scheme are the computation costs for signcrypt and unsigncrypt operations. A comparison of the efficiency of such schemes has been made against the operations involved, such as the point addition on G_1, point scalar multiplication on G_1, multiplication on G_2, pairing operation, hash operation, ciphertext size. Table 4 compares the proposed scheme with the schemes proposed in the literature with respect to the above said operations. The proposed scheme is evidently more efficient than the proposed schemes in the literature.

To the best of the authors' knowledge there is only one ring signcryption scheme [20] for wireless sensor networks. The analysis proves that the proposed scheme is more efficient than the existing one. The proposed scheme has a significant advantage over the most influential scheme. The scheme has improved in terms of the ciphertext size and point multiplication. In the case of sensor networks, the running time and energy consumption basically depend upon two factors: the number of pairings and number of point multiplications. The formulae for the running time and energy consumption can be taken from [25], as shown in Fig. 1.

According to [25], the computation time for pairing of MICA2 and Tmote Sky is 10.96 sec and 5.25 sec, respectively. Similarly, the computation time for point multiplication of MICA2 and Tmote Sky is 2.16 sec and 1.04 sec, respectively. The voltage level is assumed to be 3V and the current draw for MICA2 and Tmote Sky is 7.86 and 3.45 mA respectively. Table 5 presents the calculated running time and energy consumption for Z. Qi et al.'s scheme [20] and the proposed scheme. Fig. 2 shows the



(a) (b)

Fig. 2. Performance of the proposed scheme with respect to Z. Qi's Scheme (a) Running Time (s), (b) Energy Consumption (mJ).

performance of the proposed scheme with respect to Z.Qi et al.'s scheme as the number of nodes in the ring increases.

8. Conclusion

Wang et al. [26] proved that Zhu et al.'s scheme [13] is insecure against anonymity and also does not satisfy the property of unforgeability. Selvi el al. [19] also attacked and proved the scheme prone to confidentiality attack. Until now, very few ID-based ring signcryption schemes have been proposed and most have been proven to be insecure. In this paper, an efficient ID based ring signcryption scheme was presented, which has been proven to be secure against the primitive properties of signcryption: confidentiality, unforgeability and anonymity. This paper included an analysis of existing schemes and calculated results of the proposed scheme for wireless sensor networks. Future work may include ring signcryption schemes in combination with ID-based threshold signcryption, ID-based proxy signcryption and ID-based hybrid signcryption schemes and certificate-less schemes in the standard model. In addition, constant ciphertext size ring signcryption schemes can be improved to reduce the communication overhead.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarsubramaniam and E. Cayirci, "Wireless Sensor Networks: a survey," Computer Networks, vol. 38, no. 4, pp 393-422, 2002. Article (CrossRef Link)

[2] S. Olariu, "Information Assurance in Wireless Sensor Networks," Sensor network research group, Old Dominion University, IEEE Computer Society. 2006. Article (CrossRef Link)

[3] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," Computer Networks, vol. 52, no. 12, pp 2292-2330, 2008. Article (CrossRef Link)

[4] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," *Proc. CRYPTO '84, LNCS,* vol. 196, pp. 47-53, Springer-Verlag, 1984. Article (CrossRef Link)

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proc. CRYPTO '01, LNCS*, vol. 2139, pp. 213-229, Springer-Verlag, 2001. Article (CrossRef Link)

[6] R. L. Rivest, A. Shamir and Y. Tauman, "How to Leak a Secret," *Proc. Advances in Cryptology in Asiacrypt 2001, LNCS*, vol. 2248, pp. 552-565, Springer-Verlag, 2001. Article (CrossRef Link)

[7] F. Zheng and K. Kim, "Id-based blind signature and ring signature from pairings," *Proc. Advances in cryptology Asiacrypt 02, LNCS*, vol. 2501, pp. 533-547, Springer-Verlag, 2002. Article (CrossRef Link)

[8] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption)," *Proc. Advances in Cryptology - CRYPTO-97*, pp 165–179, 1997. Article (CrossRef Link)

[9] J. Baek, R. Steinfeld, and Y. Zheng, "Formal Proofs for the Security of Signcryption," *Proc. PKC - 02, LNCS*, vol. 2274, pp.81-98, 2002. Article (CrossRef Link)

[10] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world," *Proc. Advanced Information Networking and Applications-AINA 05*, pp. 649-54, Taipei, Taiwan, 2005. Article (CrossRef Link)

[11] X. Y. Huang, F. T. Zhang and W. Wu, "Identity-based ring signcryption scheme," *Proc. Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 34, no. 2, pp. 263–266, February 2006.

[12] L. Wang, G. Zhang and C. Ma, "A Secure Ring Signcryption Scheme for Private and Anonymous Communication" *Proc. Int. Conf. Network and Parallel Computing-Workshops*, 2007. Article (CrossRef Link)

[13] Z. Zhu, Y. Zhang and F. Wang, "An efficient and provable secure identity based ring signcryption scheme," *Proc. Computer Standards & Interfaces*, pp. 649-654, 2008. Article (CrossRef Link)

[14] L. Zhu and F. Zhang, "Efficient identity based ring signature and ring signcryption schemes," *Proc. Int. Conf. on Computational Intelligence and Security, CIS '08*, vol. 2, pp. 303–307, December 2008. Article

(CrossRef Link)
[15] F. Li, H. Xiong and Y. Yu, "An Efficient ID-based ring signcryption scheme," *Proc. Int. Conf. Communications, Circuits and Systems-ICCCCAS'08*, pp. 542-546,Xiamen, China, 2008. Article (CrossRef Link)
[16] F. Li, M. Shirase and T. Takagi, "Analysis and improvement of authenticatable ring signcryption scheme," *Proc. Int. Conf. ProvSec-08, Proc. Journal of Shanghai Jiaotong University (Science)*, pp. 679–683, 13-6, December 2008. Article (CrossRef Link)
[17] Y. Yu, F. Li, C. Xu and Y. Sun, "An efficient identity-based anonymous signcryption Scheme," *Proc. Wuhan University Journal of Natural Sciences*, vol. 13, no. 6, pp. 670– 674, December 2008. Article (CrossRef Link)
[18] J. Zhang, S. Gao, H. Chen and Q. Geng, "A novel id-based anonymous signcryption scheme," *Proc. APWeb/WAIM, LNCS*, 5446, pp 604–610, Springer, 2009. Article (CrossRef Link)
[19] S. S. D. Selvi, S. S. Vivek and C. P. Rangan, "On the security of identity based ring signcryption schemes," *Proc. 12th Int. Conf. ISC'09*, Pisa, Italy, September 7-9, 2009, *Proc. LNCS,* vol. 5735, pp 310–325, Springer, 2009. Article (CrossRef Link)
[20] Z. Qi, G. Yang, X. Ren and Y. Li, "An ID-Based ring Signcryption scheme for Wireless Sensor Networks," *Proc. IET Int. Conf. Wireless Sensor Network'10*, Beijing, China, pp. 368–373, Nov. 2010. Article (CrossRef Link)
[21] S. S. D. Selvi, S. S. Vivek, C. P. Rangan, "Identity Based Ring Signcryption with Public Verifiability," *Proc. Int. Conf. on SECRYPT'10*, 2010. Article (CrossRef Link)
[22] M. Zhang, Y. Zhong, B. Yang and W. Zhang, "Analysis and improvement of an ID-based anonymous signcryption model" *Proc. ICIC (1), LNCS*, vol. 5754, pp. 433–442, Springer, 2009. Article (CrossRef Link)
[23] J. Zhou, "An Efficient Identity-Based Ring Signcryption Scheme without Random Oracles," *Proc. Int. Conf. Computer and Electrical Engineering 4th (ICCEE – 11)*, 2011.
[24] J. Malone-Lee, "Identity based signcryption," *Proc. Cryptology, ePrint Archive, Report 2002/098*, 2002. Article (CrossRef Link)
[25] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier and R. Dahab "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor networks," EWSN 2008, Bologne, Italy, LNCS 4913, pp. 305-320, Springer-Verlag 2008. Article (CrossRef Link)
[26] H. Wang and H. Yu, "Cryptanalysis of Two Ring Signcryption Schemes," *Proc. Inscrypt'08, LNCS*, vol. 5487, pp 41-46, Springer-Verlag, 2009. Article (CrossRef Link)
[27] G. Sharma, S. Bala and A. K. Verma, "An Identity-Based Ring Signcryption Scheme," Proc. IT Convergence and Security 2012, LNEE, vol. 215, pp. 151-157, 2013. Article (CrossRef Link)

Gaurav Sharma received his M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. He received his M. Sc. and B. Sc. degrees from CCS University, Meerut, India. He is pursuing a Ph. D from Thapar University, Patiala, India.

Suman Bala received her M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. She had received her B-Tech degree from Punjab Technical University, Jalandhar, India. She is pursuing a Ph. D from Thapar University, Patiala, India.

A. K. Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001, respectively, majoring in Computer Science and Engineering. He worked as Lecturer at M.M.M. Engg. College, Gorakhpur from 1991 to 1996. From 1996 he has been associated with the same University. He has been a visiting faculty to many institutions. He has published more than 100 papers in referred journals and conferences (India and Abroad). He is a member of various program committees for different International/National Conferences and is on the review board of various journals. He is a senior member (ACM), LMCSI (Mumbai). He is a certified software quality auditor by MoCIT, Govt. of India. His current research interests include wireless networks, routing algorithms and securing ad hoc networks.

Copyrights © 2013 The Institute of Electronics Engineers of Korea